

Chatterbox Services, Inc.
Compliance Professionals

Electronic Filing through ECFS

Marlene H. Dortch
Office of the Secretary
Federal Communications Commission
445 12th St. S.W.
Washington, DC 20554

February 20, 2012

Re Telekom Malaysia (USA), Inc. Annual Customer Proprietary Network
Information Compliance Certification; EB Docket No. 06-36

Dear Ms. Dortch:

Please find the attached Annual Customer Proprietary Network Information
("CPNI") Compliance Certification for Telekom Malaysia (USA), Inc. for year end 2011.
Please call me if you have any questions regarding this filing.

Sincerely,



Hope Halpern, Esq.
hope@chatterboxsvs.com

Encls.
cc: BCPI

**Annual 47 C.F.R. S: 64.2009(e) CPNI Certification of Telekom Malaysia (USA) Inc.
for 2011**

EB Docket 06-36

Date filed: February 20, 2012

Form 499 Filer ID: 825447

Name of signatory: Hafiz Lockman

Title of signatory: Director

I, Hafiz Lockman, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. S: 64.2001 et seq.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 et seq. of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed


Hafiz Lockman

**STATEMENT REGARDING OPERATING PROCEDURES IMPLEMENTING 47 C.F.R.
SUBPART U GOVERNING THE USE OF CUSTOMER PROPRIETARY NETWORK
INFORMATION ("CPNI")**

Telekom Malaysia-USA Inc. ("TM-USA"), has established policies and procedures to assure compliance with Part 64 of Title 47 of the Code of Federal Regulations, Subpart U – Customer Proprietary Information ("CPNI") § 64.2001 et. seq. of the Commission's rules.

TM-USA operates solely as a provider of wholesale international services. TM-USA does not provide any services to end-user customers in the United States, and TM-USA does not permit CPNI to be used in its sales and marketing efforts. Nonetheless, TM-USA has implemented the following CPNI use, notice, authentication, and security procedures to ensure compliance with the Commission's rules.

I. Notice Required For Use of CPNI

TM-USA has not provided notification to its customers and has not asked for approval to use CPNI because TM-USA does not use CPNI outside of the areas that are allowed without customer approval. TM-USA does not share customers CPNI with any joint venture partner, independent contractor or any other third party. ***In the event that at a future time TM-USA decides to use CPNI in a manner that requires customer approval, it will do so in accordance with the approval and notice requirements specified in 47 CFR §§ 64.2007- 64.2008 of the Commission's rules.***

II. Safeguards on the Disclosure of Customer Proprietary Network Information.

TM-USA has procedures in place to assure that customers are properly authenticated prior to disclosing CPNI. TM-USA will properly authenticate a customer prior to disclosing CPNI as follows:

15.4

(a) **In person** – the customer must be personally known by the employee or the customer must provide a valid photo ID matching the customer's account information.

(b) **Telephone access to CPNI.** TM-USA will only disclose call detail information over the telephone, based on customer-initiated telephone contact, if the customer first provides TM-USA with a password, as described in paragraph (d) below that is not prompted by the carrier asking for readily available biographical information, or account information. If the customer does not provide a password, TM-USA will only disclose call detail information by sending it to the customer's address of record, or by calling the customer at the telephone number of record. If the customer is able to provide call detail information to TM-USA during a customer-initiated call without TM-USA's assistance, then TM-USA may discuss the call detail information provided by the customer.

(c) **Online access to CPNI.** TM-USA will authenticate a customer without the use of readily available biographical information, or account information, prior to allowing

the customer online access to CPNI related to a telecommunications service account. Once authenticated, the customer may only obtain online access to CPNI related to a telecommunications service account through a password that is not prompted by TM-USA asking for readily available biographical information, or account information.

(d) Establishment of a Password and Back-up Authentication Methods for Lost or Forgotten Passwords. To establish a password, TM-USA must authenticate the customer without the use of readily available biographical information, or account information. TM-USA may create a back-up customer authentication method in the event of a lost or forgotten password, but such back-up customer authentication method may not prompt the customer for readily available biographical information, or account information. If a customer cannot provide the correct password or the correct response for the back-up customer authentication method, the customer must establish a new password as described in this paragraph.

(e) Notification of account changes. TM-USA will promptly notify customers immediately whenever a password, customer response to a back-up means of authentication for lost or forgotten passwords, online account, or address of record is created or changed. This notification may be through a voicemail or text message sent by TM-USA to the telephone number of record, or by mail to the address of record, and will not reveal the changed information or be sent to the new account information.

(f) Wholesale Customers – at this time TM-USA has no retail end user customers and only provides wholesale carrier-to-carrier services in the United States. TM-USA and its wholesale carrier customers address issues of CPNI protection specifically in their contracts, and these may or may not differ somewhat from the authentication procedures identified in paragraphs (a) through (e) above. TM-USA's wholesale customers each have a dedicated account representative.

III. Notification of Customer Proprietary Network Information Security Breaches.

In the case of a breach, TM-USA will as soon as practicable, and in no event later than seven (7) business days, after reasonable determination of the breach, electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) through the FCC link at <http://www.fcc.gov/eb/cpni>.

(a) Notify customers only after 7 full business days have passed after notification to the USSS and the FBI unless the USSS or FBI has requested an extension.

(b) If there is an extraordinarily urgent need to notify affected customers or the public sooner in order to avoid immediate and irreparable harm, it will be done only after consultation with the relevant investigating agency. TM-USA shall cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.

(c) Maintain a record of any breaches discovered, notifications made to the USSS and the FBI and notifications made to customers. The record will include if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach. TM-USA shall retain the record for a minimum of 2 years.

(d) Include a summary of the breach in the annual compliance certificate filed with the FCC.

IV. Record Retention

TM-USA shall retain all information regarding CPNI. Following are the minimum retention periods TM-USA has established:

- CPNI notification and records of approval if used – five years
- Marketing campaign if used – one year
- Breaches: five years
- Annual Certification – five years
- Employee training certification – five years
- All other information – two years.